FAQ and Support

Cisco Defense Orchestrator Platform Maintenance Schedule

Cisco Defense Orchestrator Maintenance Schedule

CDO updates its platform every week with new features and quality improvements. Updates can be made during a 3 hour period according to this schedule.

Most often, updates are completed on Thursday, but the Friday and Sunday maintenance windows are used if necessary.

Table 1: CDO Maintenance Schedule

Day of the Week	Time of Day (24-hour time)
Thursday	09:00 UTC - 12:00 UTC
Friday	09:00 UTC - 12:00 UTC
Sunday	09:00 UTC - 12:00 UTC

During this maintenance period, you can still access your tenant and if you have a cloud-delivered Firewall Management Center, you can access that platform as well. Additionally, the devices you have onboarded to CDO continue to enforce their security policies.

Note We advise you not to use CDO to deploy configuration changes on the devices it manages during maintenance periods.

If there is a failure that stops CDO or cloud-delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible even if it is outside the maintenance window.

Cloud-delivered Firewall Management Center Maintenance Schedule

Customers who have a cloud-delivered Firewall Management Center deployed on their tenant are notified approximately 1 week before CDO updates the cloud-delivered Firewall Management Center environment. Super-admin and Admin users of the tenant are notified by email. CDO also displays a banner on its home page notifying all users of upcoming updates.

The update to your tenant may take up to 1 hour and occurs within the 3 hour maintenance period on the maintenance day assigned to your tenant's region. While your tenant is being updated, you will not be able to access the cloud-delivered Firewall Management Center environment, but you will still be able to access the rest of CDO.

Table 2: Cloud-delivered Firewall Management Center Maintenance Schedule

Day of the Week	Time of Day (24-hour time)	Region
Wednesday	04:00 UTC - 07:00 UTC	Europe, the Middle East, or Africa (EMEA)
Wednesday	17:00 UTC - 20:00 UTC	Asia-Pacific-Japan (APJ)
Thursday	09:00 UTC - 12:00 UTC	Americas

How CDO Processes Personal Information

To learn how Cisco Defense Orchestrator processes your personal identifiable information, see the Cisco Defense Orchestrator Privacy Data Sheet.

Complete the Initial Configuration of a Secure Firewall Threat Defense Device Using the CLI

Connect to the device's CLI to perform initial setup, including setting the management IP address, gateway, and other basic networking settings using the setup wizard. Ensure all DNS and firewall ports are accessible for communication.

The dedicated management interface is a special interface with its own network settings. If you do not want to use the management interface, you can use the CLI to configure a data interface instead.

Before you begin

This procedure applies to the following scenarios:

- The Firepower 1000, Firepower 2100, Secure Firewall 3100, and ISA 3000 models.
- This configuration is ideal for devices that going to be onboarded with their CLI registration key.

Note Do **not** use this configuration procedure for devices that are onboarding with low-touch provisioning.

Procedure

Step 1 Connect to the device's CLI, either from the console port or using SSH to the management interface. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

For Firepower 1000, Firepower 2100, Secure Firewall 3100 models: The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

(Firepower 1000/2100, Secure Firewall 3100) At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the FXOS troubleshooting guide for the reimage procedure.See the reimage guide for instructions.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3 (Firepower 1000/2100, Secure Firewall 3100) If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the device, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference.

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Note The management interface settings are used even when you enable threat defense access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—If you want to use a data interface for threat defense access instead of the management interface, choose **manual**. Although you do not plan to use the management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface**—If you want to use a data interface for threat defense access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **YES** to configure the device for the device to be managed by either the cloud-delivered Firewall Management Center or Secure Firewall device manager.

  Manage the device locally?—Enter **NO** to configure the device for remote management with the on-prem management center.
- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface threat defense access is only supported in routed firewall mode.

Step 5 (Optional) Configure a data interface for management center access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command. See About Data Interfaces for more informatio.

- The original management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the management interface gateway to **data-interfaces**, this command will set it now.

- When you onboard the device for FTD management through CDO, CDO discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. You can later make changes to the access interface configuration, but make sure you don't make changes that can prevent the device or CDO from re-establishing the management connection. If the management connection is disrupted, the device includes the **configure policy rollback** command to restore the previous deployment.
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  Also, local DNS servers are only retained if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in CDO, including the DNS servers, to match the device configuration.
- You can change the management interface after you onboard the threat defense for FTD management through CDO, to either the management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6 (Optional) Limit data interface access to CDO on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.